



TRUST CENTER · RECHTSDOKUMENT

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (AVV) nach Art. 28 DSGVO

Muster · Stand: 02.10.2026

zwischen

dem Kunden gemäß Hauptvertrag – nachfolgend „Verantwortlicher“ –

und

EFINITI Services GmbH, c/o Neuwerker Business Office, Dammer Straße 136-138, 41066 Mönchengladbach, vertreten durch den Geschäftsführer Sascha Norbert Kirchhofer, Amtsgericht Mönchengladbach HRB 24012 – nachfolgend „Auftragsverarbeiter“ –

1. Gegenstand und Dauer

- 1.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Bereitstellung der Plattform „Pandora“ (KI-gestützte Agenten, Kommunikation, Dokumentenverarbeitung) nach dem zwischen den Parteien geschlossenen Vertrag (nachfolgend „Hauptvertrag“).
- 1.2 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags.

2. Art, Zweck und Umfang der Verarbeitung

- 2.1 Art der Verarbeitung: Speichern, Organisieren, Auslesen, Abfragen, Verwenden, Übermitteln an Subprozessoren, Pseudonymisieren, Löschen.
- 2.2 Zweck: Erbringung der Leistungen nach dem Hauptvertrag.
- 2.3 Art der Daten: Stamm- und Kontaktdaten, Kommunikationsinhalte, vom Verantwortlichen hochgeladene Dokumente und deren Inhalte, Nutzungs- und Protokolldaten.
- 2.4 Kategorien betroffener Personen: Beschäftigte und Beauftragte des Verantwortlichen, deren Kunden, Lieferanten und sonstige Kommunikationspartner.

- 2.5** Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nur zulässig, wenn der Verantwortliche dies gesondert mitteilt und die Parteien zusätzliche Maßnahmen vereinbaren.

3. Weisungsbefugnis

- 3.1** Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats hierzu verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). In diesem Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
- 3.2** Weisungen erfolgen in Textform. Der Hauptvertrag und die Konfiguration der Plattform durch den Verantwortlichen gelten als Weisung.
- 3.3** Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 S. 3 DSGVO).

4. Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

5. Sicherheit der Verarbeitung

- 5.1** Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 (TOM-Übersicht) beschrieben sind.
- 5.2** Die Maßnahmen dürfen fortentwickelt werden, sofern das Schutzniveau nicht unterschritten wird.

6. KI-spezifische Regelungen

- 6.1** Personenbezogene Daten werden vor der Übermittlung an ein KI-Modell pseudonymisiert.
- 6.2** Der Auftragsverarbeiter nutzt Daten des Verantwortlichen nicht zum Training von KI-Modellen und schließt dies auch gegenüber Subprozessoren vertraglich aus.
- 6.3** Bei Modellanbietern wird eine Speicherung der Anfragen ausgeschlossen (Zero Data Retention), soweit in Anlage 2 angegeben.

7. Weitere Auftragsverarbeiter (Subprozessoren)

- 7.1** Der Verantwortliche erteilt seine allgemeine Genehmigung zum Einsatz der in Anlage 2 aufgeführten Subprozessoren.

- 7.2** Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorab in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung. Der Verantwortliche kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, ist der Verantwortliche berechtigt, den Hauptvertrag hinsichtlich der betroffenen Leistungen außerordentlich zu kündigen.
- 7.3** Der Auftragsverarbeiter erlegt jedem Subprozessor dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO). Er haftet für dessen Pflichtverletzungen wie für eigene.
- 7.4** Eine Übermittlung in ein Drittland erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (einschließlich EU-US Data Privacy Framework) oder der EU-Standardvertragsklauseln.

8. Unterstützung des Verantwortlichen

- 8.1** Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO). Anträge, die direkt bei ihm eingehen, leitet er unverzüglich weiter.
- 8.2** Er unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen.
- 8.3** Verletzungen des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.

9. Löschung und Rückgabe

Nach Beendigung des Hauptvertrags gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück oder löscht sie, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO). Einzelheiten regelt der Exit- und Portabilitätsprozess. Datensicherungen werden im Rahmen des regulären Sicherungszyklus überschrieben, spätestens nach 90 Tagen.

10. Nachweise und Kontrollen

- 10.1** Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung, insbesondere aktuelle Zertifikate der Subprozessoren und Prüfberichte.
- 10.2** Der Verantwortliche ist berechtigt, Überprüfungen einschließlich Inspektionen nach rechtzeitiger Anmeldung (in der Regel 14 Tage) während der üblichen Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchzuführen (Art. 28 Abs. 3 lit. h DSGVO). Für Finanzkunden gelten ergänzend die Regelungen der DORA-Vertragsklauseln.

11. Haftung

Die Haftung richtet sich nach Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

12. Schlussbestimmungen

12.1 Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

12.2 Änderungen bedürfen der Textform. Es gilt deutsches Recht.

Anlage 1: Technische und organisatorische Maßnahmen

Anlage 2: Liste der Subprozessoren

Ort, Datum · Verantwortlicher

Ort, Datum · EFINITI Services GmbH